Digital *Signatures* Initiative:
Business and Technology Horizons Report

November 2001

Prepared for

The Commonwealth of Virginia
Council on Technology Services Digital Signatures Workgroup

By

The Digital Signature Initiative Horizons Team

DIGITAL SIGNATURES INITIATIVE HORIZONS TEAM REPORT CONTRIBUTORS:

TEAM MEMBERS

David Bunn
Network Manager
Department of Motor Vehicles

Craig Goeller
Data Processing Operations Manager
Department of Medical Assistance Services

Deborah Dodson
Acting Assistant Commissioner for Technology
Department of Motor Vehicles

Ray Lindquist
Vice President
Parikh Advanced Systems
Representing Virginia Department of Transportation

Shirley Payne, Chair
Director, Security Coordination and External Relations
University of Virginia

Nelly Romero
Project Manager
Department of Medical Assistance Services

Marge Sidebottom
HIPAA Coordinator & Emergency Preparedness Chair
University of Virginia Hospital

OTHER CONTRIBUTORS

Carol M. Longley, Federal and State Legislative Tracking
Senior Policy Analyst, Governmental Relations
Department of Motor Vehicles

Timothy M. Sigmon, Ph.D., Technical Advisor
Director, Advanced Technology
University of Virginia

INTRODUCTION

As the Commonwealth of Virginia pursues strategies for implementing digital signature capabilities for its agencies, localities, and educational institutions, it is important to leverage the learning and expertise of others pursuing similar goals. To this end, the Business Horizons Team, operating under the direction of the Commonwealth of Virginia Digital Signatures Implementation (DSI) Workgroup, was formed in November 2000. This team serves as the primary point of contact to explore and incorporate national and international models, programs, and initiatives that may provide opportunities for mutually beneficial partnerships with the Federal government, other jurisdictions, and organizations, including those providing educational and health care services. In July 2001 this team also assumed responsibility for tracking new technologies and standards related to Public Key Infrastructure (PKI) and was renamed the DSI Horizons Team.

This report summarizes the team's activities and findings thus far.

KEY LEARNING POINTS

_ Although technological developments in the area of PKI have not been significant in the past year, there has been great emphasis on determining the practical aspects of the technology and putting it to use.

_ Establishing a secure PKI environment is decidedly not a trivial undertaking; different security needs require different solutions. A survey of companies, industry associations and individuals undertaken in Singapore in early 2001 highlighted obstacles to PKI implementation that will likely have to be overcome by the Commonwealth as well:

- General lack of awareness (education)
- Cost and complexity of deployment and maintenance
- Issues related to ease of use and convenience
- Lack of demand and killer applications
- Impact on performance of applications
- Lack of interoperability standards for cross-border certification
- Lack of consensus on cross-border legal issues

While cross-border issues mentioned in the last two items are especially important for smaller countries such as Singapore, they are also important for the Commonwealth when considered in the context of cross-state and agency-to-agency activities.

_ There are a growing number of opportunities for Virginia state agencies, businesses and citizens to use Federal Government issued ACES certificates for transacting business with federal agencies. We believe there is also great potential to partner with selected federal agencies to allow VOLT certificates to be used in place of ACES certificates.

- There is also the potential for future collaboration between the Commonwealth and the National HealthKey Program, which is working on developing the architecture to secure electronic transactions among healthcare entities. This program is currently being reconstituted to embrace other industries as well.

- A key to government-led reengineering and reinvention efforts has been card-based systems and services, including, and in particular, smart card systems.

- In the near future the use of digital signatures will likely become a requirement for doing business in the handling of protected health information (PHI). This action will affect state agencies that handle such data, especially agencies in the Health and Human Resource Secretariat.

INTERNATIONAL SCENE

Significant digital signature efforts are underway in many countries across the globe. The European Union and its members show a great deal of activity, as do several Asian and South American states. Most are working on putting the necessary legal frameworks in place before embarking on technology implementations, although practical implementations of digital signature technology are also underway in several countries.

One of the more ambitious projects in Europe is a seven-country initiative that sets out to develop electronic management of different municipal services and transactions between citizens, small and medium enterprises, and administrations. The integrity and authentication of document-flow between the public administration and citizens will be guaranteed through this service in accordance with international technical standards and law. Planned services fall into four wide categories:

1. General municipal services to citizens that could be defined as "Public Information Services".
2. Mobility, environmental and emergencies services that could be defined as "Urban Management Applications".
3. The complex transactions between citizens and local administrations - including multi-purpose payment means (smart cards) - that could be defined as "Public Transaction Services".
4. Educational, social and cultural underlying services for students, disabled and elderly people, and interested citizens, that could be defined as "Cultural Services".

The Italian province of Brescia is one of the first among participating government entities to issue and manage free electronic certificates to citizens in its municipalities.

Collaborative electronic commerce efforts between countries are being actively pursued as well. A notable example is the signing of a joint statement between the United Kingdom and Canada in February 2001 acknowledging their shared vision and

confirming their intent to cooperate in the fields of e-commerce and e-government. Ministers representing the two countries, using Canadian secure digital technologies, signed the statement.

An issue, which raises considerable debate at the international level, concerns the liability aspects of an open PKI. Some countries, notably the EU, Malaysia, and Singapore, believe that allowing certificate authorities to limit their liability is a pre-requisite for widespread use of electronic authentication. Others, however, feel that such limitations are unnecessary or premature. Lack of consensus between countries may slow adoption of international standards.

NATIONAL SCENE

FEDERAL GOVERNMENT ACTIVITIES

There has also been significant digital signature-related activity at the national level, especially within the Federal Government. The major driver of the federal effort is the 1998 Government Paperwork Elimination Act (GPEA), which requires federal agencies to offer electronic alternatives to current paper-based forms by October 2003. GPEA specifies that electronic signatures cannot be deemed illegal or invalid solely on the basis that they are electronic. The act, therefore, establishes the incentive and the legal basis for moving forward with investigation of digital signatures.

The objective of the federal initiative is to build efficient, cost-effective processes, using digital signature technology where appropriate. These processes are currently being organized around communities of interest, such as citizen groups, and business partners.

Parties leading the effort are:

- The General Services Administration – specifically, the Office of Government-wide Policy, the Federal Technology Service Office, and the Access Certificates for Electronic Governments (ACES) Program.
- The Federal PKI Steering Committee, which reports to the CIO Council.

The primary means by which the Federal Government will support adoption of digital signature technology are the ACES Program and the Federal Bridge Certification Authority (FBCA).

The ACES Program enables the Federal Government to issue a single key for their customers, although there are no restrictions in place that preclude more than one certificate being issued to a given customer. There are four types of certificates: root, individual, business, and agency. There is only one ACES assurance level, although agencies are themselves able to raise the level of assurance on an application-by-application basis. Any federal agency may participate in the ACES Program. These

agencies may also authorize non-federal agencies with which they partner to be issued ACES certificates.

A number of federal agencies began to use ACES certificates this year. In fact, Virginia's Department of Environmental Quality (DEQ) is currently participating in an ACES certificate-based program offered by the Environmental Protection Agency (EPA). Through that program, the DEQ will be able to electronically submit reports to the EPA, a process which previously required hard signatures.

Work over the past two years to establish the Federal Bridge Certification Authority (FBCA) was completed this summer. The FBCA provides the mechanism by which agencies may cross-verify certificates issued by differing trust domains. This bridge concept has captured the interest of a number of industries, e.g. health care and higher education, and efforts are underway to develop industry-specific bridges and mechanisms to connect them to the Federal Bridge.

Federal agency applications in which digital signatures are or will soon be used were analyzed by the DSI Workgroup's Horizons Team for relevance to Virginia agencies, businesses and citizens. A list of applications that warrant tracking in the future is provided in Appendix A.

CROSS-STATE INITIATIVES

In late 2000 the National Governors Association and the National Electronic Commerce Coordinating Council partnered to address state-to-state interoperability and other issues concerning interstate commerce. Committees were formed to study the following areas:

- Interoperability
- Legal
- Policy
- Security and Privacy

To date these committees have not issued any final reports or recommendations; however, working drafts of the following deliverables are currently circulating among members:

1. "Framework for Electronic Signature Reciprocity" - an education piece on risks and levels of trust.
2. "Record Retention Analysis under E-Sign" - addresses Federal E-Sign legislation's impact on the authority of states to require that private parties retain written records of certain transactions
3. "Consumer Privacy Protections on the Internet" - addresses current laws and trends.
4. A side-by-side comparison of e-signature and UETA legislation.
5. A certificate policy template.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA), better known as the Kennedy-Kassebaum Bill, was signed into law on August 21, 1996. The "Portability" portion deals primarily with continuation of health insurance coverage and provides for the wavier of pre-existing conditions of health insurance coverage when persons move to a new employer. During the Senate committee sessions on the bill, a section on Administrative Simplification was amended into the original bill for the "Accountability" portion. The Administrative Simplification provisions require that the Secretary of the Federal Department of Health and Human Services (FDHHS) develop national uniform regulations dealing with standardization of virtually every facet of electronic commerce related to health care. These proposed regulations include:

- security of electronic health information and electronic signatures;
- privacy of such protected identifiable information;
- standardization of electronic data interchange formats of transactions and codes;
- national provider identifier, and
- national employer identifier.

The proposed and final rules apply to any health plan, any health care clearinghouse, and any health care provider that electronically maintains or transmits health care information relating to an individual. It will require all U.S. health care organizations that transmit or store electronic or paper messages or records pertaining to individual patients (including providers, insurers, and health care clearinghouses) to prevent the unauthorized disclosure of such information, while also ensuring easy access for authorized users and approved purposes

On April 14, 2001, the FDHHS issued the HIPAA Privacy Regulation in final form. It focuses on policies and procedures protecting individuals' rights and their protected health information, and audit trails of disclosures. Some methods being discussed to protect protected health information include encryption, use of secure e-mail and public key infrastructure. Currently, the use of electronic digital signature is optional, but is encouraged. Also, HIPAA statute requires FDHHS to issue an electronic signature standard. At this time, there are discussions at FDHHS that the electronic digital signature portion of the security regulations may become mandatory. Virginia's agencies that must comply with the HIPAA Regulations would be affected by this requirement.

There are two HIPAA related efforts currently under way that either support digital signature and public key infrastructure, or are reviewing it as an option for consideration. First, the National Medicaid EDI HIPAA (NMEH) Claims Attachment Sub workgroup is doing analysis on and writing a business use case for electronic transmission of signatures on claims attachments. The purpose of their document is to define the health care industry's business need to capture signatures within an electronic transaction and outline the various possible means to convey this information. The document does not address the technical issues but does focus on the business need and use case for conveyance of signatures electronically.

Their challenge is to find a cost-effective mechanism to capture signature data while meeting the federal requirements. The NMEH workgroup is investigating signature on file, scanned image, digital signatures, point of service swipe cards, SMART cards, and biometrics alternatives to receive and capture signature data. At this time it appears that the NMEH workgroup will support the first two options because they are the most cost effective and least resource intensive methods for implementing signature requirements.

The next effort is with the Drug Enforcement Administration (DEA). They are expected to issue a proposed regulation by March 2002 allowing the electronic prescription of controlled substances if providers use PKI to secure their digital signatures. DEA has done extensive investigation PKI and how it can be used in processing prescriptions for controlled substances electronically. More information on this subject can be found at their web site at:

http://www.deadiversion.usdoj.gov/ecomm/e_rx/overview/index.html

The DEA is not entering new territory with its work on PKI. NIST (National Institute of Standards and Technology), one of the lead agencies in developing a digital standard for the federal government, has based its work on PKI in recent years. The standard is known as the Federal Information Processing Standard, or FIPS, 186. To find this and other listings of NIST Information Technology Standards, visit their web site at:

http://www.nist.gov/public_affairs/standards.htm#Information

Also, H.R. 1259 was passed by the House of Representatives and would require NIST to work with the private sector to establish voluntary interoperability standards for PKI systems.

In the near future the use of digital signatures will likely become a requirement for doing business in the handling of PHI. This action will affect state agencies that handle such data, especially agencies in the Health and Human Resource Secretariat.

INTERESTING DEVELOPMENTS IN OTHER STATES

Among states, Washington appears to lead others in rollout of digital signature applications, although Illinois is not far behind. Both states want businesses and citizens to be able to conduct transactions with state and local agencies using a single, state-branded certificate. They each began issuing certificates in limited areas this year. There are implementation differences, however, and these are summarized in the table that follows.

	Washington	*Illinois*
Planned Use	citizen to government, business to government, business to business, and citizen to citizen	Initial focus is government to government and business to government. Will consider citizen to government in the future
Certificate Authority	Digital Signature Trust	Illinois Dept. of Central Management Services (CMS)
PKI Vendor	Digital Signature Trust	Entrust
Certificate Assurance Levels	standard intermediate high	high only *(possible expansion later)*
Cost Model	Annual users' fee. Amount varies based upon assurance level.	No cost to citizens and businesses. General revenue fund is used to buy the certificates. CMS will bill other state agencies for CA services.

Another development is that a number of states, including New Jersey, Georgia, California, Washington and Illinois, are reportedly interested in including interoperability with the Federal Bridge Certificate Authority in their PKI strategies. Illinois in particular is interested in cross-certifying with the Federal Bridge and may be the first to test this capability.

LEGAL DEVELOPMENTS

The question of who owns property when it is converted from the original format into an electronic medium has been in the forefront of several cases before both the lower and upper federal courts. The decisions in these cases have the potential to rewrite contract law, in that the courts are finding that contracts and agreements to publish material in traditional media do not automatically extend to electronic media. The U.S. Supreme Court ruled in July that publishers must pay independent contributors when their work, first published in traditional print media, is subsequently published electronically. The 11th U.S. Court of Appeals ruled that the National Geographic Society violated copyright law by publishing photographs in a CD-ROM format without gaining specific permission from the photographer.

Consumer privacy issues, especially as they relate to identity theft, continue to raise concerns among lawmakers. The 107th Congress in particular introduced a large number of bills to restrict the ability of government and business to require personal information from customers. Many of these bills would prohibit the collection, use and dissemination of social security numbers (SSN's), and reflect a number of different approaches to SSN privacy:

- Prohibit the Social Security Administration from releasing the numbers and place severe restrictions on their use;
- Prohibit any federal, state, or local jurisdiction from requiring (whether mandatory or voluntary) customers to provide it;
- Criminalize collection and release of SSN's without consent;
- Prohibit use of SSN on driver's licenses.

At the same time, the 107th Congress continues to push for legislation that will smooth the way for wider use and acceptance of electronic commerce. It has begun to address the digital divide in the U.S, and several bills have been submitted that would provide funding and grants to rural areas and those who will make technology investments in such areas.

One final issue that will continue to occupy lawmakers and courts alike concerns profits and taxes: The ability of states and localities to collect taxes on Internet businesses. For states faced with shrinking revenues, Internet taxes are a potential windfall. Those with Internet businesses argue that a tax structure to collect revenue for all states would be cumbersome and restrictive. This issue is complex and multi-dimensional, and will likely be decided slowly through litigation in determining taxation authority.

A list of recent court rulings and legislation related to e-government can be found in Appendix B.

TECHNOLOGY DEVELOPMENTS

In general, fundamental technological developments in the area of PKI have not been significant in the past year, although innovative product developments based upon the technology are evident. The Digital Signature Initiative Workgroup has benefited this year from a number of vendor presentations aimed at keeping the group apprised of new products and successful uses of PKI technology. These presentations are listed in Appendix C.

As noted, emphasis has been on determining the practical aspects of the technology and putting it to use, and one example we wish to highlight is in the use of smart cards. Smart card activities, as well as obstacles to use, are described below.

SMART CARD INITIATIVES

It appears from our research that a key strategy being adopted for government reengineering and reinvention efforts is card-based systems and services, including, and in particular, smart card systems. These systems have been presented as an effective vehicle for portable access control, storing private information, and securing access and communications through cryptographic boundaries. In addition to performing the general function of verifying an individual's identity, smart cards are being implemented for

secure facilities access, secure network access, secure Internet purchasing, secure communications, and secure electronic document processing.

Examples of specific smart card pilots and production use we have seen are:

1. replacement of traditional drivers licenses with smart cards (initiatives at this point are outside the U.S.),
2. police cars equipped with terminals for smart card driver's licenses, allowing on the spot recording of traffic violations and fine payment (again, outside the U.S. at this point),
3. smart card terminals incorporated into kiosks allowing for identification of the user and for debiting of service fees,
4. hospitals using smart card terminals for medical information cards, and
5. welfare agencies using smart cards for benefit dispersal,
6. smart card-based passports,
7. use of smart cards for immigrant identification.

Two of the largest smart card initiatives in the U.S. are being conducted by the General Services Administration (GSA) and the Department of Defense. The Presidential Budget for Fiscal Year 1998 stated: "The Administration wants to adopt smart card technology so that, ultimately, every [Federal] employee will be able to use one card for a wide range of purposes, including travel, small purchases, and building access." To this end, GSA has partnered with private industry to develop an open, interoperable specification to ensure smart cards an agency purchases from one vendor will work with applications and smart-card readers used by another agency. The Department of Defense has undertaken a separate effort to issue multiple application smart cards to four million people, including active duty military personnel, reservists, civilian Pentagon employees and contractors.

Smart card efforts are also underway in the banking industry with several leading banks such as American Express, VISA, Citicorp, Chase Manhattan Corp., and Wachovia having conducted pilot testing and/or released chip based smart cards. For information on the National Automated Clearinghouse smart card pilot, see the "Collaboration Activity" section below.

These and other interesting smart card initiatives are described in Appendix D.

OBSTACLES TO SMART CARD ADOPTION

International actions over the past year indicate that concerns about personal privacy and the ability to protect consumer information and transactions will be the next major issue that has to be resolved before wide spread acceptance of electronic commerce can be found. As a result, adoption of smart cards, especially in the guise of national identity cards, has been below expectations in some countries. Civil liberties concerns in the United Kingdom are expected to delay rollout of the technology. Comments from industry representatives and analysts indicate that "*the importance placed upon an individual's single digital identity has too high a value to be encapsulated within a single*

card" (A. Kellet, senior research analyst, Butler Group) and that "*people are too nervous to have everything on the same card*" (G. Lisimaque, CIO, Gemplus).

Despite these concerns, smart card adoption in Europe and other countries has occurred much more rapidly than in the United States. From the technological point of view, the existence of a widely used credit card infrastructure within the United States, coupled with the significant effort and expense required to install smart card readers has made adoption within this country far less than anticipated. Computer networks are so fast and inexpensive that even the smallest purchase is now electronically verified by the card-issuing bank. According to a VISA spokesman, "our telecommunications costs are low and our fraud rate, knock on wood, have been so low that the rationale for the chip card has never existed."

A survey to measure the use of smart cards in the United States and Canada will be conducted by KPMG LLP with results of the initial phase to be presented at the New York-based Smart Card Alliance's Annual Meeting October 9 to 12.

OTHER TRENDS AND BEST PRACTICES

In addition to smart cards, we have been monitoring for other trends and best practices as well. Two worth noting are the assignment of registration authority responsibilities and a ground-breaking e-government, incubator-like program in the State of Washington.

REGISTRATION AUTHORITIES

Initiatives underway in Singapore, Hong Kong, as well as the United States show potential for involving national Post Offices as Registration Authorities.

Boston-based Imagitas, in partnership with the U.S. Postal Service, aims to offer secure, authentic, and binding online transactions between individuals and government agencies through the GovKey program. GovKey is a national digital certificate program with in-person authentication designed to accelerate adoption of e-Government for secure transactions between the public and government. USPS will act as Registration Authority, provide investigative activity through its Postal Inspection Service, and oversee and evaluate the overall program.

WASHINGTON ACADEMY

In support of its aggressive move toward digital government, the State of Washington has established an innovative "Washington Academy," which assists state agencies and localities in jumpstarting digital signature and other e-government applications. The DSI Workgroup held a conference call with Academy representatives on April 6, 2001 and was very much impressed with the progress the organization has made and its vision for the future. The Academy's charter was created in December 1999, along with a general

process aimed at obtaining tangible results. Within three months the Academy's first session was held.

The Academy's managers found no models for what they intended to accomplish; however, one early decision they made was to follow the metaphor of academic research universities and to use university terms, such as course, and syllabus. In their case, though, the intent was not to teach traditional classes, but to build actual applications as part of the sessions. The Academy is financially supported in part through a tuition charge to each participating agency.

The Academy's approach is to develop templates and guidelines, not standards, for state agencies to follow. The decision on whether or not to adopt these templates and guidelines is left up to the agencies. The Academy's philosophy is that if people see something working, they will use it.

Academy staff members work with key stakeholders in the state to determine priorities for service class development. Once a service class, such as electronic licensing, has been selected, state agencies propose specific projects to be addressed through the Academy. These are screened for affinity with other projects, and the surviving ones are undertaken as case work for the Academy "course" sessions. Representatives from the agencies proposing these projects participate in the sessions. Coursework involves defining a common vision for the end product, defining requirements that best meet the needs of participants, writing code, and developing templates and guidelines that can be reused by other agencies.

At the time of the conference call, the Academy had completed templates and guidelines for permit processes and e-forms.

COLLABORATION ACTIVITY

Meetings and conference calls with a number of other entities over the past year have provided much good information and advice, which can be leveraged as the CoVa DSI effort moves forward. In a few cases the opportunity for future collaboration has been identified. Brief descriptions of the contacts made follows, along with an indication of future collaboration potential.

U.S. General Services Administration

A meeting was held on November 7, 2000 with representatives from the U.S. General Services Administration (GSA) to develop a common understanding of digital signature strategies of the Federal Government and how these may impact entities in each and citizens served by both. As mentioned in the National Scenes section of this report, the two primary strategies at the federal level are the ACES Program and the Federal Bridge Certificate Authority. Details of these strategies were shared in the meeting, and the GSA offered the following in the way of assisting Virginia in pursuing its own strategies:

- Many lessons have been learned in putting together the ACES Program that may be applicable to the VOLT Program, e.g. information that should be included in certificate policies and contracts. GSA is willing to share their experiences with Virginia.

- Virginia was invited to attend the monthly Federal PKI Steering Committee meetings.

- Virginia was invited to attend a "Defending Cyberspace 2000" conference sponsored by GSA. Three representatives from the CoVa DSI Workgroup accepted this invitation and found the seminars and workshops very useful.

- There are several federal agencies currently seeking state partners for their digital signature applications. In addition to the Environmental Protection Agency, with which Virginia is already working on a state reporting application, FEMA and the Social Security Administration are particularly interested in state partners for piloting annual reporting applications.

Since this meeting, the DSI Workgroup has conducted an analysis of federal agencies known to be implementing digital signature applications and the relevance of these applications to Virginia agencies, businesses and citizens. This analysis is documented in Appendix A.

DEPARTMENT OF DEFENSE & VIRGINIA'S DMV

The Department of Defense (DoD) is aggressively deploying chip-based smart cards to all military and civilian personnel. The card will eventually be used for multiple purposes, including physical access to secure areas, network authentication, and digital signing. Because of the large number of military personnel within the Commonwealth, the DSI Workgroup (the Division of Motor Vehicles specifically) decided to pursue the idea of allowing the DoD smart card to be used in lieu of a DMV-issued PIN number to perform secure transactions from DMV kiosks in the Pentagon and elsewhere. Initially, the DoD was quite interested in the concept, but in the end a DoD policy that restricts use of the card to only DoD activity halted work on the project. The DSI Workgroup may pursue this idea, however, with other smart card-issuing federal agencies, such as the Veterans Administration.

MAJOR BANK

On March 23, 2000 the DSI Workgroup met with a major banking organization to explore the potential value of a standard multi-application smart card for CoVa employees and to learn from the bank's experience with smart card deployment. Bank representatives liked the overall approach the Commonwealth is taking with regard to

digital signing, especially the idea of issuing standard VOLT certificates for identity purposes. In their view, building a good business case for smart cards in the U.S. may be more difficult than it has been abroad, where there is massive fraud and the communications infrastructure that currently supports online financial transactions in the U.S. is not already in place.

Should we pursue smartcards further, bank representatives strongly advise us to:
1. Integrate the smart card reader with the swipe reader and deliver both to users as one package.
2. Focus initially on just one smart card application that provides value. Implement that successfully, and then move on to another.
3. Keep things as simple as possible. For example, use of biometrics adds a significant layer of complexity because of consumer acceptance issues.

NATIONAL AUTOMATED CLEARING HOUSE (NACHA) INTERNET COUNCIL

A conference call was held with NACHA on March 2, 2001 to discuss a pilot that organization is facilitating to develop a process allowing consumers to use Internet enabled ATM/debit cards to make Internet-initiated debit payments from their checking accounts. This pilot which ended on April 13, 2001, successfully processed 598 transactions in which digital signatures substituted for personal identification numbers. Results were published in July 2001 on the http://internetcouncil.nacha.org web site. NACHA characterized the pilot as successful and stated in it's report's conclusion that *"The ISAP (Internet Secure ATM Payments) Pilot met its success criteria, achieved its objectives, and demonstrated that it is feasible to use the ISAP process to support Internet-initiated ATM/debit card payments"*. The DSI Workgroup will study NACHA's final report in detail and will analyze the pilot results for relevance to the CoVa effort.

NATIONAL HEALTHKEY PROGRAM

A conference call was held on May 4, 2001 with the program manager of the National HealthKey Program. This program is a collaboration of five states (Washington, Utah, Minnesota, North Carolina, and Massachusetts) to pilot test architecture to enable secure electronic transactions among healthcare entities. A bridge-style architecture was chosen for this program, and that bridge is now operational. The first application is secure, digitally signed email.

Key lessons learned the manager passed on were to:
1. Keep the certificate policy simple.
2. Issue identity certificates only.
3. Do not use extensions fields in the certificates.

The potential for future collaboration between the Commonwealth and this effort appears to be strong. The DSI Workgroup's contact with the Program was timed right at the

point when the initial members were evaluating pilot results and considering options for expansion, not just to include healthcare organizations in other states, but also to encompass organizations in other industries. The program manager expressed interest in involving Virginia in its future plans and will be back in touch with us as soon as the program is ready to move forward.

COLLABORATIONS AMONG COVA STATE AGENCIES

In addition to pursuing partnership opportunities with external entities, the DSI Workgroup has held exploratory sessions concerning collaboration opportunities among selected state agencies. For example, Virginia Tech has proposed the idea of having the Division of Motor Vehicles serve as a producer and distributor of "Hokie Passport" smart cards the school hopes to issue to all Virginia Tech students. As Virginia Tech continues its emphasis on delivering instruction using distance learning methods, the number of students taking courses from locations far from Blacksburg will increase. DMV's many offices scattered throughout the state could be leveraged to put smart cards in the hands of these distance learners.

Another example is the possibility of using secure, digitally signed email to exchange sensitive healthcare related data between the University of Virginia and the Department of Medical Assistance Services. UVa and DMAS are currently exploring the potential in this area.

PKI IMPLEMENTATION & ADMINISTRATION ISSUES

While our research shows evidence of successful PKI implementations and also opportunities for the Commonwealth of Virginia to leverage those successes, our observations also lead to the conclusion that it can be a daunting task to move beyond understanding the available technology to the point of having a PKI structure installed and functioning. There are many solution approaches to choose among and each choice that is made opens up some futures and closes others. Making these choices is a prediction of how the use of PKI will evolve in a given business area. Once implemented, it is difficult to change course.

Some key choices that have to be addressed deal with the issues of:

- Insuring the integrity of the private key, yet providing extraordinary customer assistance for mishaps.
- Providing support for roaming users: How do we give access from anywhere without leaving a footprint, and administer certificate replacement without calling the users in?
- Developing standards for a Commonwealth CP and CPS. Do we, for example, archive revoked certificates for the interval that the Commonwealth archives documents?

- Determining where the CA resides: Should we outsource (employing service level agreements and liability statements) or use in-house services (maintaining internal staff skills to detect and respond to security vulnerabilities before they are exploited and providing disaster recovery)?

In order for Commonwealth agencies to define what the needs for a PKI infrastructure are, it seems advisable to tighten the scope from how the infrastructure might ultimately work, to what is required now. These specific targets will help define the user interaction needs. In essence, our research reaffirms the vision and guiding principles set forth in the September 2000 Digital Signature Initiative Workgroup Report, which focused on the need for "simplicity of the 'cleanest,' least complicated and most flexible technology and policy solutions."